REMARKS/ARGUMENTS

Reconsideration of the application is requested.

Claims 1-13 remain in the application. Claims 1-13 have been amended.

In item 1 on page 2 of the above-identified Office action, claims 7-8 have been rejected as being indefinite under 35 U.S.C. § 112, second paragraph.

More specifically, the Examiner has stated that the term "may have" in claim 7 is indefinite. The word "may" has been deleted.

It is accordingly believed that the claims meet the requirements of 35 U.S.C. § 112, second paragraph. Should the Examiner find any further objectionable items, counsel would appreciate a telephone call during which the matter may be resolved. The above-noted changes to the claims are provided solely for cosmetic and/or clarificatory reasons. The changes are neither provided for overcoming the prior art nor do they narrow the scope of the claims for any reason related to the statutory requirements for a patent.

In item 2 on page 2 of the above-mentioned Office action, claims 1-9 have been rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

More specifically, the Examiner has stated that the claims recite a method for performing a mathematical function.

Claims 1-9 have been limited to a method of modular multiplication within a cryptographic algorithm, which results in a limitation to a practical application, in order to overcome the non-statutory rejection. The support may be found on page 1, line 15 and page 2, line 12 of the specification.

In item 3 on pages 2-3 of the above-mentioned Office action, claims 1-13 have been rejected as being unpatentable over Sedlak (US 4,870,681) in view of Walter ("Faster Modular Multiplication by Operand Scaling," Editor: Feigenbaum, J.: "Advances in Cryptology-CRYPTO '91," Springer Verlag, August 1991, pp.313-323) under 35 U.S.C. § 103(a).

The rejection has been noted and claims 1 and 13 have been amended in an effort to even more clearly define the invention of the instant application. Support for the changes is found on page 9, lines 18-21, and page 17, lines 15-17, 32, and 35 of the specification.

Before discussing the prior art in detail, it is believed that a brief review of the invention as claimed, would be helpful.

Claim 1 calls for, inter alia:

> iteratively working off the modular multiplication using the multiplication look-ahead process and the reduction look-ahead process and utilizing the transformed modulus so as to obtain at the end of the iteration a transformed result for the modular multiplication, the predetermined fraction of the transformed modulus being used in the reduction look-ahead process; and
>
> re-transforming the transformed result by modular reduction of the transformed result utilizing the modulus.

Claim 10 calls for, inter alia:

> a processor for iteratively working off the modular multiplication using the multiplication look-ahead process and the reduction look-ahead process and utilizing the transformed modulus so as to obtain at the end of the iteration a transformed result for the modular multiplication, the predetermined fraction of the transformed modulus being used in the reduction look-ahead process; and
>
> a re-transformer for re-transforming the transformed result by modular reduction of the transformed result utilizing the modulus.

Sedlak, besides not disclosing the transforming step as admitted by the Examiner, also does not disclose the step of iteratively working off, and specifically, the amended feature that the predetermined fraction of the transformed modulus is used in the reduction look-ahead process. In Sedlaak, only the predetermined fraction of the non-transformed modulus is used. Furthermore, Sedlak only teaches using the normal modulus rather than the transformed modulus. Finally, Sedlak also does not disclose the step of retransforming the transformed result by modular reduction of the transformed result utilizing the modulus (and not the transformed modulus).

Walter does not disclose the usage of a multiplication look-ahead process and a reduction look-ahead process. Although Walter discloses scaling a modulus by a factor f such that f multiplied by the modulus has its q most significant digits fixed, Walter does not disclose anything about the scaling factor, in particular, about the nature or characteristic of the q most significant fixed digits as outlined in the first paragraph of section on page 316 of Walter.

In contrast, according to the invention of the instant application, the transforming number, which is used for multiplying the modulus, is calculated using the modulus such that a predetermined fraction of the transformed modulus has a higher-order digit with a first predetermined value followed by at least one lower-order digit having a second <u>different</u> predetermined value.

While Walter teaches using any factor f so that the most significant digits of the modulus are fixed, the invention of the instant application is defined so that the transforming number is calculated with respect to a predetermined fraction of the transformed modulus rather than the modulus itself in the prior art. More specifically, in the invention of the instant application the transforming number is calculated so that the predetermined fraction of the transformed modulus has a very specific bit-pattern, i.e., that a higher-order digit such as the most significant bit has a first value such as 1, and that this bit is followed by one or more bits (at least one lower-order digit), which have a second different value such as 0s.

In addition, Walter does not disclose the step of iteratively working off using the multiplication look-ahead process and the reduction look-ahead process, and does not disclose the use of the predetermined fraction of the transformed modulus in the reduction look-ahead process.

Finally, Walter also does not disclose the retransforming step.

In summary, the invention of the instant application does not merely generally define a scaled modulus as is the case in Sedlak. Instead, a very specific scaled modulus, namely a modulus in which a predetermined fraction thereof has a higher-order digit with a first predetermined value followed by at least one lower-order digit having a second different predetermined value, is used in the invention of the instant application.

Claim 2 of the instant application recites a very easy calculation of the reduction shift value used in the reduction look-ahead process in which only number of digits between the higher-order digit with the first predetermined value of the transformed modulus and the highest-order digit of the intermediate result having the first predetermined value has to be counted. This results in a highly simplified ZDN comparison, which is much more cumbersome in Selak.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claims 1 and 10. Claims 1 and 10 are, therefore, believed to be patentable over the art and since all of the dependent claims are ultimately dependent on claims 1 or 10, they are believed to be patentable as well.

In view of the foregoing, reconsideration and allowance of claims 1-13 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate a telephone call so that, if possible, patentable language can be worked out.

If an extension of time for this paper is required, petition for extension is herewith made. Please charge any fees which might be due with respect to 37 CFR Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,

Yonghong Chen

Yonghong Chen
Reg. No. 56,150

For Applicants

YC

December 14, 2005

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101